BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam era teknologi informasi, berbagai aktivitas bisnis dan komunikasi tak lepas dari peran teknologi informasi, terutama aktivitas yang menggunakan jaringan internet. Akses yang luas terhadap internet mempermudah proses pengelolaan dan pertukaran data, tetapi juga meningkatkan risiko keamanan data, terutama untuk informasi pelanggan yang bersifat sensitif [1]. Seiring dengan berkembangnya teknologi, resiko berupa ancaman terhadap privasi dan keamanan data semakin meningkat yang dapat menyebabkan pencurian informasi hingga kerugian operasional dari suatu perusahaan [2].

Berdasarkan data dari Susanto et al. (2023), terdapat lebih dari 60% perusahaan di Indonesia membutuhkan sistem keamanan yang lebih kuat untuk melindungi data digital mereka [3]. Pernyataan tersebut diperkuat dengan data penelitian Prayuti (2024) bahwa dalam tiga tahun terakhir, terdapat peningkatan serangan siber pada sektor industri layanan internet sebesar 45% [2]. Selain itu, laporan dari Forbes Advisor (2023) menyebutkan bahwa setiap 14 detik sebuah perusahaan menjadi korban serangan *ransomware* secara global, dengan peningkatan insiden serangan siber sebesar 72% sejak tahun 2021 [4]. Indonesia sendiri menempati posisi ke-8 dalam jumlah kebocoran data tertinggi secara global, dengan lebih dari 820 ribu kasus pembobolan yang tercatat pada kuartal II tahun 2022 [5]. Data ini menggarisbawahi perlunya penguatan keamanan digital, terutama dalam melindungi data pelanggan dari ancaman yang terus berkembang.

Ancaman keamanan digital yang terus meningkat ini tidak hanya menjadi perhatian bagi perusahaan besar, tetapi juga berdampak pada perusahaan kecil dan menengah, termasuk penyedia layanan internet seperti Ardi Hotspot yang berada di Kecamatan Jogoroto, Kabupaten Jombang. Adapun untuk perusahaan ini mengandalkan pencatatan data pelanggan dan

akun autentikasi PPPoE *(Point-to-Point Protocol over Ethernet)* pelanggan menggunakan sistem berbasis *website* yang terintegrasi dengan sistem manajemen perangkat *server.* Berdasarkan hasil wawancara dengan pengelola ISP "Ardi Hotspot," sistem manajemen data pelanggan yang digunakan saat ini belum memiliki perlindungan enkripsi, sehingga informasi seperti kredensial *login* PPPoE dan identitas pengguna sangat rentan terhadap perubahan manual tanpa autentikasi karena tersimpan dalam bentuk *plaintext*. Bahkan, pernah terjadi serangan pada sistem yang menyebabkan hilangnya seluruh data konfigurasi internet pelanggan yang tersimpan di *server*, dimana terdapat 500 data pelanggan yang terdampak langsung atas insiden tersebut. Serangan ini tidak hanya mengakibatkan kebocoran data, tetapi juga membuat sistem yang terintegrasi dengan perangkat *server* mengalami gangguan parah hingga operasional layanan ISP sempat terhenti selama hampir satu minggu. Fakta ini menunjukkan adanya kebutuhan mendesak untuk merancang dan mengimplementasikan sistem manajemen data yang aman dan terenkripsi sebagai solusi nyata terhadap permasalahan yang dihadapi pada studi kasus ini.

Sebagai solusi, penelitian ini bertujuan untuk merancang sistem manajemen data pelanggan berbasis *website* yang menggunakan *framework* Next.js dan basis data MongoDB Atlas yang berbasis awan *(cloud)* untuk menangani permasalahan tersebut. Sistem ini mengimplementasikan algoritma enkripsi RSA, yang diharapkan dapat meningkatkan keamanan data pelanggan dari akses tidak sah serta memberikan autentikasi *login* yang lebih aman bagi *admin* dan karyawan. RSA adalah algoritma kriptografi asimetris yang menggunakan pasangan kunci publik dan kunci privat untuk mengamankan data. Algoritma ini sangat diandalkan dalam keamanan digital karena tingkat keamanannya bergantung pada kompleksitas faktorisasi bilangan besar. Keunggulan algoritma ini meliputi kemampuan untuk memberikan otentikasi yang kuat, kerahasiaan data, serta perlindungan yang efektif terhadap akses tidak sah [6].

Harapannya, penerapan enkripsi RSA pada sistem manajemen data pelanggan ini akan memberikan tingkat keamanan yang lebih baik dalam melindungi data pelanggan dari akses yang tidak sah dan mengoptimalkan efisiensi operasional pada perusahaan Ardi Hotspot dalam pengelolaan data pelanggan.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini yakni bagaimana cara mengimplementasikan algoritma kriptografi RSA pada sistem manajemen data pelanggan berbasis web untuk memastikan keamanan data pelanggan dan data akses manajemen *server* dari ISP "Ardi Hotspot" dari potensi akses tidak sah.

1.3. Tujuan Penelitian

Adapun penelitian ini memiliki tujuan yang ingin dicapai, yaitu menerapkan algoritma enkripsi RSA dalam sistem manajemen data pelanggan berbasis web untuk ISP "Ardi Hotspot" guna melindungi data pelanggan dari potensi kehilangan serta meminimalisir akses autentikasi yang tidak sah ke dalam sistem.

1.4. Batasan Masalah

Agar penelitian ini lebih terfokus dan efektif, penelitian ini dibatasi pada pengembangan sistem yang mencakup fitur-fitur utama, yaitu pengelolaan data pelanggan, pengelolaan data akun autentikasi PPPoE berupa *username* dan *password*, serta integrasi dengan sistem manajemen perangkat *server*. Selain itu, sistem ini juga dirancang untuk mendukung autentikasi *admin* maupun karyawan guna memastikan keamanan akses ke dalam sistem.

1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan solusi digital yang dapat meningkatkan keamanan, kecepatan, dan efisiensi dalam pengelolaan data pelanggan, sehingga dapat mengurangi risiko kerusakan data dan mempercepat pemulihan layanan ISP “Ardi Hotspot” ketika terjadi gangguan. Selain itu, implementasi algoritma kriptografi RSA diharapkan mampu melindungi data pelanggan dari potensi ancaman keamanan seperti kebocoran data dan akses yang tidak sah. Dengan sistem yang lebih terstruktur dan aman, ISP "Ardi Hotspot" juga dapat meningkatkan kepercayaan pelanggan serta memperkuat citra perusahaan sebagai penyedia layanan internet yang andal dan modern. Penelitian ini tidak hanya bermanfaat bagi perusahaan, tetapi juga memberikan referensi berharga bagi pengembangan sistem manajemen data berbasis kriptografi di bidang lain.